

**PENERAPAN ALGORITMA PRESENT UNTUK ENKRIPSI DATA PADA
SENSOR *INTERNET OF THINGS* MENGGUNAKAN WOKWI DAN
NODE-RED**

SKRIPSI



**UIN SUNAN AMPEL
S U R A B A Y A**

Disusun Oleh:

**YUNA IKBAR ZAIDAN
09010622015**

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL
SURABAYA
2026**

PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini,

Nama : Yuna Ikbar Zaidan

NIM : 09010622015

Program Studi : Sistem Informasi

Angkatan : 2022

Menyatakan bahwa saya tidak melakukan plagiat dalam penulisan skripsi saya yang berjudul: "PENERAPAN ALGORITMA PRESENT UNTUK ENKRIPSI DATA PADA SENSOR INTERNET OF THINGS MENGGUNAKAN WOKWI DAN NODE-RED". Apabila suatu saat nanti terbukti saya melakukan tindakan plagiat, maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 11 Maret 2026
Yang menyatakan,

A handwritten signature in black ink is written over a red meter stamp. The stamp features the Garuda Pancasila emblem and the text 'METERAI TEMPEL' and 'BBANX252345535'.

METERAI
TEMPEL
BBANX252345535

(Yuna Ikbar Zaidan)
NIM. 09010622015

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh:

Nama : YUNA IKBAR ZAIDAN


NIM : 09010622015

Judul : PENERAPAN ALGORITMA PRESENT UNTUK ENKRIPSI DATA
PADA *INTERNET OF THINGS*

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 16 Oktober 2025

Dosen Pembimbing 1


(Muhammad Ardik Izzudin, M.T.)
NIP. 198403072014031001

Dosen Pembimbing 2

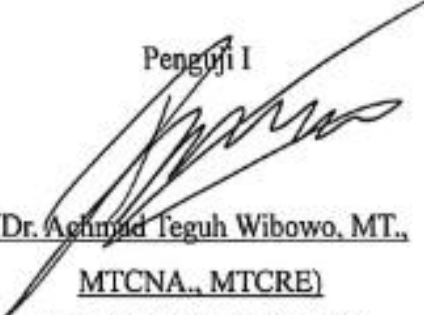

(Mujib Ridwan, M.T.)
NIP. 198604272014031004

PENGESAHAN TIM PENGUJI SKRIPSI


Skripsi Yuna Ikbar Zaidan ini telah dipertahankan
di depan tim penguji skripsi
di Surabaya, 27 Maret 2026.

Mengesahkan,
Dewan Penguji

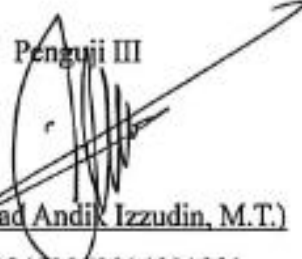
Penguji I


(Dr. Achmad Teguh Wibowo, MT.,
MTCNA., MTCRE)
NIP. 198810262014031003


Penguji II


(Andhy Permadi, M.Kom)
NIP. 198110142014031002

Penguji III


(Muhammad Andik Izzudin, M.T.)
NIP. 198403072014031001

Penguji IV


(Mujib Ridwan, M.T.)
NIP. 198604272014031004

Mengetahui,

Dekan Fakultas Sains dan Teknologi
UIN Sunan Ampel Surabaya

(Dr. Asepul Hamdani, M.Pd)
NIP. 196507312000031002

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI



**KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN**

Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama : YUNA IKBAR ZAIDAN
NIM : 09010622015
Fakultas/Jurusan : Sains dan Teknologi/Sistem Informasi
E-mail address : yunaikbar@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :

Skripsi Tesis Desertasi Lain-lain (.....)
yang berjudul :

PENERAPAN ALGORITMA PRESENT UNTUK ENKRIPSI DATA

PADA SENSOR INTERNET OF THINGS MENGGUNAKAN WOKWI

DAN NODE-RED

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Eksklusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara *fulltext* untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 12 Juni 2026

Penulis

(YUNA IKBAR ZAIDAN)

ABSTRAK

PENERAPAN ALGORITMA PRESENT UNTUK ENKRIPSI DATA PADA SENSOR *INTERNET OF THINGS* MENGGUNAKAN WOKWI DAN NODE-RED

Oleh:
Yuna Ikbar Zaidan

Perkembangan *Internet of Things* (IoT) yang pesat membawa tantangan baru dalam keamanan data, terutama karena perangkat IoT memiliki keterbatasan daya, memori, dan kapasitas komputasi yang menyulitkan penerapan algoritma enkripsi konvensional. Penelitian ini bertujuan untuk menerapkan algoritma PRESENT sebagai solusi *lightweight cryptography* pada sistem IoT, serta menguji validitas dan performanya. Objek penelitian adalah simulasi perangkat ESP32 dan sensor DHT22 pada platform Wokwi, dengan Node-RED sebagai sisi dekripsi, yang dihubungkan melalui protokol MQTT menggunakan broker Mosquitto. Algoritma PRESENT-80 diimplementasikan menggunakan MicroPython pada sisi ESP32 dan JavaScript pada sisi Node-RED. Pengujian dilakukan melalui tiga metode, yaitu uji *test vector*, uji *Avalanche Effect*, dan uji performa waktu enkripsi-dekripsi. Hasil uji *test vector* menunjukkan seluruh skenario mendapatkan nilai *PASS*, membuktikan validitas implementasi algoritma. Uji *Avalanche Effect* menghasilkan rata-rata *Hamming Distance* sebesar 31,52 bit (49,24%) yang mendekati nilai ideal 50%, menunjukkan difusi algoritma yang baik. Rata-rata waktu enkripsi pada ESP32 sebesar 1.054 milidetik dan dekripsi pada Node-RED sebesar 14 milidetik, keduanya masih dalam batas interval pengiriman yang ditentukan. Penelitian ini menyimpulkan bahwa algoritma PRESENT layak dan efisien diterapkan pada ekosistem IoT, walaupun performanya kurang baik jika dibandingkan dengan algoritma seperti AES-128-CBC dan ChaCha20 dengan lingkungan yang sama.

Kata kunci: *Internet of Things*, Algoritma PRESENT, Enkripsi Data, Wokwi, Node-RED

UIN SUNAN AMPEL
S U R A B A Y A

ABSTRACT

IMPLEMENTATION OF THE PRESENT ALGORITHM FOR DATA ENCRYPTION ON INTERNET OF THINGS SENSORS USING WOKWI AND NODE-RED

By:
Yuna Ikbar Zaidan

The rapid growth of the Internet of Things (IoT) introduces new challenges in data security, particularly because IoT devices are constrained by limited power, memory, and computational capacity, making conventional encryption algorithms difficult to apply. This study aims to implement the PRESENT algorithm as a lightweight cryptography solution for IoT systems and to evaluate its validity and performance. The research object consists of a simulated ESP32 device and DHT22 sensor on the Wokwi platform, with Node-RED serving as the decryption side, connected via the MQTT protocol using a Mosquitto broker. The PRESENT-80 algorithm was implemented using MicroPython on the ESP32 side and JavaScript on the Node-RED side. Testing was conducted through three methods: test vector validation, Avalanche Effect analysis, and encryption-decryption performance measurement. Test vector results showed that all scenarios passed, confirming the correctness of the algorithm implementation. The Avalanche Effect test yielded an average Hamming Distance of 31.52 bits (49.24%), approaching the ideal value of 50%, indicating good diffusion properties. The average encryption time on the ESP32 was 1,054 milliseconds and decryption on Node-RED was 14 milliseconds, both within the configured transmission interval. This study concludes that the PRESENT algorithm is feasible and efficient to be applied to the IoT ecosystem, although its performance is less good when compared to algorithms such as AES-128-CBC and ChaCha20 in the same environment.

Keywords: Internet of Things, PRESENT Algorithm, Data Encryption, Wokwi, Node-RED

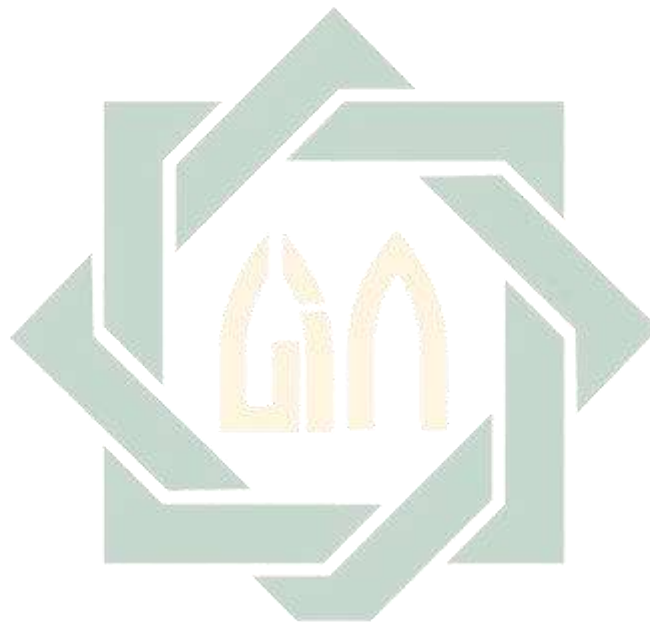
UIN SUNAN AMPEL
S U R A B A Y A

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PERSETUJUAN PEMBIMBING	ii
PENGESAHAN TIM PENGUJI SKRIPSI.....	iii
PERNYATAAN KEASLIAN.....	iv
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI.....	v
MOTTO.....	vi
HALAMAN PERSEMBAHAN	vii
UCAPAN TERIMAKASIH	viii
ABSTRAK	x
ABSTRACT.....	xi
DAFTAR ISI.....	xii
DAFTAR GAMBAR	xv
DAFTAR TABEL.....	xvii
DAFTAR LAMPIRAN.....	1
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	5
1.3 Batasan Masalah.....	5
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian	6
1.5.1 Akademik.....	6
1.5.2 Aplikatif.....	6
BAB II TINJAUAN PUSTAKA	7
2.1 Penelitian Terdahulu.....	7
2.2 Dasar Teori	12
2.2.1 IoT (<i>Internet of Things</i>).....	12
2.2.2 Definisi Kriptografi.....	14
2.2.3 Aspek Keamanan Kriptografi	16
2.2.4 Kriptografi Simetris	19
2.2.5 Kriptografi Asimetris	22

2.2.6	Kriptografi pada Perangkat IoT	24
2.2.7	Arduino Sketch	25
2.2.8	Wokwi	26
2.2.9	MicroPython.....	28
2.2.10	Node-RED.....	29
2.2.11	MQTT	31
2.2.12	<i>Lightweight cryptography</i> (LWC).....	33
2.2.13	Algoritma AES-128-CBC	34
2.2.14	Algoritma ChaCha20	34
2.2.15	Algoritma PRESENT	35
2.2.16	Analisis Keamanan Algoritma	37
2.3	Integrasi Keilmuan	38
BAB III METODOLOGI PENELITIAN.....		41
3.1	Metodologi Penelitian	41
3.2	Identifikasi Masalah	42
3.3	Studi Literatur	43
3.4	Desain Eksperimen.....	43
3.4.1	Arsitektur Sistem.....	44
3.4.2	Skenario Eksperimen	45
3.4.3	Metrik Evaluasi	49
3.5	Implementasi Eksperimen.....	50
3.6	Pengujian Eksperimen.....	51
3.6.1	<i>Test Vector</i>	51
3.6.2	<i>Avalanche Effect</i>	52
3.6.3	Performa Waktu Enkripsi dan Dekripsi	52
3.7	Evaluasi Hasil.....	53
3.8	Penarikan Kesimpulan	54
BAB IV HASIL DAN PEMBAHASAN.....		55
4.1	Hasil Penelitian	55
4.1.1	Implementasi Sisi Enkripsi (Wokwi)	55
4.1.2	Implementasi Sisi Dekripsi (Node-RED).....	57
4.2	Analisis dan Pembahasan.....	59

4.2.1 Uji <i>Test Vector</i> (Implementasi Validasi).....	59
4.2.2 Uji <i>Avalanche Effect</i>	60
4.2.3 Uji Performa Waktu Enkripsi dan Dekripsi	63
BAB V PENUTUP	68
5.1 Kesimpulan	68
5.2 Saran Pengembangan	69
DAFTAR PUSTAKA	70
LAMPIRAN.....	75

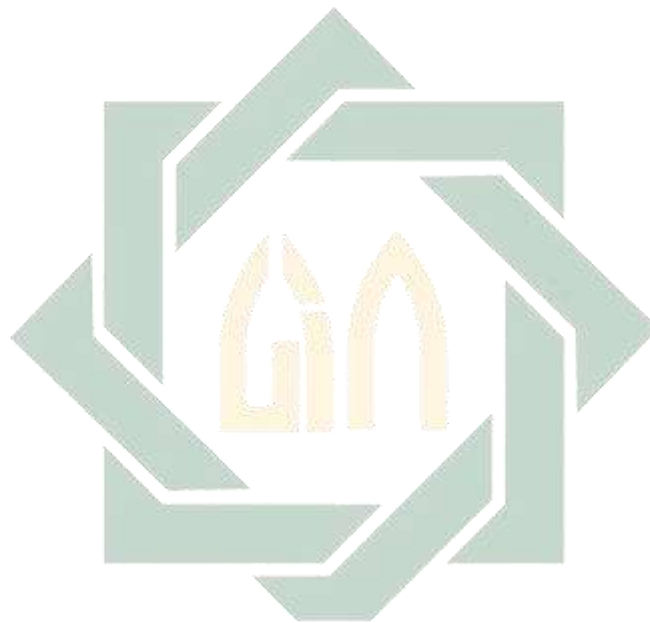


UIN SUNAN AMPEL
S U R A B A Y A

DAFTAR GAMBAR

Gambar 2.1 Proses enkripsi dan dekripsi (Sumber: Ariyus & Amikom, 2008)....	15
Gambar 2.2 Proses enkripsi dan dekripsi kriptografi simetris (Sumber: Saepulloh Aldrian, 2024)	19
Gambar 2.3 Proses block cipher (Sumber: www.tpointtech.com, 2026).....	20
Gambar 2.4 Proses stream cipher (Sumber: www.tpointtech.com, 2026)	21
Gambar 2.5 Proses enkripsi dan dekripsi kriptografi asimetris (Sumber: Basri, 2016)	23
Gambar 2.6 Tampilan halaman utama Wokwi (Sumber: www.wokwi.com, 2026)	26
Gambar 2.7 Tampilan workflow Node-RED (Sumber: flows.nodered.org, 2026) 29	
Gambar 2.8 Sistem kerja algoritma PRESENT (Sumber: Bogdanov et al., 2007) 35	
Gambar 2.9 Jaringan S/P algoritma PRESENT (Sumber: Bogdanov et al., 2007) 35	
Gambar 2.10 Tabel s-Box (Sumber: Bogdanov et al., 2007)	36
Gambar 2.11 Tabel pLayer (Sumber: Bogdanov et al., 2007)	37
Gambar 2.12 Aturan key-scheduling algoritma PRESENT (Sumber: Bogdanov et al., 2007).....	37
Gambar 3.1 Metodologi penelitian (Sumber: Wohlin et al., 2012).....	42
Gambar 3.2 Arsitektur Sistem Lingkup Komunikasi Data	44
Gambar 3.3 Skema eksperimen bagian enkripsi	45
Gambar 3.4 Pseudocode dari fungsi enkripsi algoritma PRESENT (Sumber: Bogdanov et al., 2007)	46
Gambar 3.5 Skema eksperimen bagian dekripsi	47
Gambar 3.6 Pseudocode dari fungsi dekripsi algoritma PRESENT	47
Gambar 3.7 Pemisahan Tiap Parameter Data ke dalam Dashboard.....	48
Gambar 3.8 Proses pengujian Avalanche Effect	49
Gambar 3.9 Tabel test vector (Sumber: Bogdanov et al., 2007)	51
Gambar 4.1 Diagram simulasi pada Wokwi.....	55
Gambar 4.2 Tampilan simulasi ESP32 dan DHT22 pada platform Wokwi.....	56
Gambar 4.3 Struktur payload JSON yang dikirim ke MQTT	57
Gambar 4.4 Tampilan flow Node-RED.....	57

Gambar 4.5 Tampilan dashboard Node-RED	59
Gambar 4.6 Output serial monitor Wokwi menampilkan hasil uji test vector	60
Gambar 4.7 Distribusi Hamming Distance Avalanche Effect berdasarkan bit plaintext.....	62



UIN SUNAN AMPEL
S U R A B A Y A

DAFTAR TABEL

Tabel 2.1 Penelitian terdahulu.....	7
Tabel 4.2 Hasil pengujian test vector	60
Tabel 4.3 Sampel hasil pengujian Avalanche Effect	61
Tabel 4.4 Sampel data waktu enkripsi dan dekripsi dalam milidetik.....	63
Tabel 4.5 Hasil pengukuran waktu enkripsi dan dekripsi tiga algoritma dalam milidetik	64
Tabel 4.6 Faktor teknis penentu performa ketiga algoritma	66



UIN SUNAN AMPEL
S U R A B A Y A

DAFTAR LAMPIRAN

Lampiran 1 Hasil pengujian Avalanche Test.....	75
Lampiran 2 Data waktu enkripsi dan dekripsi dalam milidetik.....	78



UIN SUNAN AMPEL
S U R A B A Y A

DAFTAR PUSTAKA

- Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A New Blockchain-Based Authentication Framework for Secure IoT Networks. *Electronics (Switzerland)*, 12(17). <https://doi.org/10.3390/electronics12173618>
- Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability (Switzerland)*, 16(23). <https://doi.org/10.3390/su162310177>
- Amin, M. M. (2016). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Jurnal Pseudocode*, 3(2).
- Arif, Z., Nurokhman, A., Studi, P., Informatika, T., & Data, K. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. 4(2), 394–405.
- Ariyus, D., & Amikom, U. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi. <https://books.google.co.id/books?id=3SSTJONEmX0C>
- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
- Bagaskoro, C., & Kuspranoto, A. H. (2023). Perancangan Simulasi Kalkulator Indeks Masa Tubuh Berbasis Arduino Uno Dan Simulasi Wokwi. *Medika Trada*, 4(2), 29–34. <https://doi.org/10.59485/jtemp.v4i2.39>
- Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., & Poschmann, A. (2007). *PRESENT: An Ultra-Lightweight Block Cipher*. 450–466.
- Dan, E. S. P., Bot, A., Athallah, Y., & Agung, R. (2022). Rancang Bangun Prototype Monitoring Lampu Jalan Secara Otomatis Menggunakan Mikrokontroler. *VIII(1)*, 12–19.
- Edwar Jacinto, G., Holman Montiel, A., & Fernando Martínez, S. (2017). Implementation of the cryptographic algorithm “present” in different microcontroller type embedded software platforms. *International Journal of Applied Engineering Research*, 12(19), 8092–8096.

- Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure Medical Data Transmission Model for IoT-Based Healthcare Systems. *IEEE Access*, 6(March), 20596–20608. <https://doi.org/10.1109/ACCESS.2018.2817615>
- Evans, D. (2011). Internet of things: How the Next Evolution of the Internet Is Changing Eveything. *Smart Power Distribution Systems: Control, Communication, and Optimization*, April, 11.
- Fadhil, M. S., Farhan, A. K., & Fadhil, M. N. (2021). A lightweight aes algorithm implementation for secure iot environment. *Iraqi Journal of Science*, 62(8), 2759–2770. <https://doi.org/10.24996/ij.s.2021.62.8.29>
- Fahmi, A., & Indra Kurniawan. (2025). Studi Kinerja Transmisi Data Menggunakan ESP32 dan Raspberry Pi Pico Berbasis Simulasi Wokwi. *Journal Zetroem*, 7(1), 80–87. <https://doi.org/10.36526/ztr.v7i1.5102>
- Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors (Basel, Switzerland)*, 16(10), 1–44. <https://doi.org/10.3390/s16101644>
- Gou, Q., Yan, L., Liu, Y., & Li, Y. (2013). Construction and Strategies in IoT Security System. *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, 1129–1132. <https://doi.org/10.1109/GreenCom-iThings-CPSCoM.2013.195>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
- Gusmeroli, S., Haller, S., Harrison, M., Kalaboukas, K., Tomasella, M., Vermesan, O., & Wouters, K. (2009). Vision and challenges for realizing the internet of things. In *Proceedings of the 3rd STI Roadmapping Workshop* (Vol. 1, Issue APRIL).
- Imdad, M., Ramli, S. N., & Mahdin, H. (2022). An Enhanced Key Schedule Algorithm of PRESENT-128 Block Cipher for Random and Non-Random

- Secret Keys. *Symmetry*, 14(3), 1–22. <https://doi.org/10.3390/sym14030604>
- Indrajati, D., & Ashari, W. M. (2025). Evaluation of the Effectiveness of Lightweight Encryption Algorithms on Data Performance and Security on IoT Devices. *Journal of Applied Informatics and Computing*, 9(3), 642–650. <https://doi.org/10.30871/jaic.v9i3.9256>
- Kusyanti, A., Agrahita Wiguna, I. P., & Andri Bakhtiar, F. (2023). Implementasi Algoritme Spongengent sebagai Algoritme Hashing untuk Integritas pada Modul Komunikasi Lora. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 10(6), 1311–1318. <https://doi.org/10.25126/jtiik.2023107119>
- Li, F., Zheng, Z., & Jin, C. (2016). Secure and efficient data transmission in the Internet of Things. *Telecommunication Systems*, 62(1), 111–122. <https://doi.org/10.1007/s11235-015-0065-y>
- Martinez Santa, F., Jacinto, E., & Montiel, H. (2019). *PRESENT Cipher Implemented on an ARM-Based System on Chip* (pp. 300–306). https://doi.org/10.1007/978-981-32-9563-6_31
- Maswadi, K., Ghani, N. B. A., & Hamid, S. B. (2020). Systematic Literature Review of Smart Home Monitoring Technologies Based on IoT for the Elderly. *IEEE Access*, 8, 92244–92261. <https://doi.org/10.1109/ACCESS.2020.2992727>
- Medina-Pérez, A., Sánchez-Rodríguez, D., & Alonso-González, I. (2021). An Internet of Thing Architecture Based on Message Queuing Telemetry Transport Protocol and Node-RED: A Case Study for Monitoring Radon Gas. *Smart Cities*, 4(2), 803–818. <https://doi.org/10.3390/smartcities4020041>
- Mestiri, H., Barraji, I., Saidani, T., & Machhout, M. (2024). A PRESENT Lightweight Algorithm High-Level SystemC Modeling using AOP Approach. *Engineering, Technology and Applied Science Research*, 14(5), 16772–16777. <https://doi.org/10.48084/etasr.8417>
- Mhaibes, H. I., Abood, M. H., & Farhan, A. K. (2022). Simple Lightweight Cryptographic Algorithm to Secure Imbedded IoT Devices. *International Journal of Interactive Mobile Technologies*, 16(20), 98–113. <https://doi.org/10.3991/ijim.v16i20.34505>
- Mishra, B., & Kertesz, A. (2020). The Use of MQTT in M2M and IoT Systems: A

- Survey. *IEEE Access*, 8, 201071–201086.
<https://doi.org/10.1109/ACCESS.2020.3035849>
- Mouha, N. (2015). The Design Space of Lightweight Cryptography. *NIST Lightweight Cryptography Workshop 2015*, 1–19.
<https://eprint.iacr.org/2015/303.pdf>
- Preview, T. S. (2012). *INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Lightweight cryptography Block ciphers iTeh STANDARD iTeh STANDARD PREVIEW. 2012.*
- Primadya, N. D., Nugraha, A., Luthfiarta, A., & Fahrezi, S. Y. (2024). Optimasi Logistic Regression untuk Deteksi Serangan DoS pada Keamanan IoT. *Jurnal Eksplora Informatika*, 13(2), 245–252.
<https://doi.org/10.30864/eksplora.v13i2.1065>
- Putri, W. E., Dewanta, F., & Afianti, F. (2022). Analisis Perbandingan Block Cipher Simon-Speck, Simeck, Skinny pada Komunikasi Berbasis LoRa. *Multinetics*, 8(2), 97–104. <https://doi.org/10.32722/multinetics.v8i2.4821>
- Sabri, O., Al-Shargabi, B., Abuarqoub, A., & Hakami, T. A. (2025). A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. *Internet of Things*, 6(2), 1–26.
<https://doi.org/10.3390/iot6020023>
- Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, 44, 100467.
<https://doi.org/10.1016/j.cosrev.2022.100467>
- Shahzad, K., Khan, S. A., & Iqbal, A. (2024). Factors influencing the adoption of Internet of Things (IoT) in university libraries: a systematic literature review (SLR). *Electronic Library*, 42(2), 255–287. <https://doi.org/10.1108/EL-07-2023-0174>
- Shamala, L. M., Zayaraz, G., Vivekanandan, K., & Vijayalakshmi, V. (2021). Lightweight cryptography algorithms for internet of things enabled networks: An overview. *Journal of Physics: Conference Series*, 1717(1).
<https://doi.org/10.1088/1742-6596/1717/1/012072>
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: The road ahead. *Computer Networks*, 76, 146–

164. <https://doi.org/10.1016/j.comnet.2014.11.008>

- Taj, S., Imran, A. S., Kastrati, Z., Daudpota, S. M., Memon, R. A., & Ahmed, J. (2023). IoT-based supply chain management: A systematic literature review. *Internet of Things (Netherlands)*, 24(October), 100982. <https://doi.org/10.1016/j.iot.2023.100982>
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in software engineering* (Vol. 236). Springer.
- Wulandari, A., Ramadhani, E. H., Fathurahman, M., & Hikmaturokhman, A. (2024). Implementation Analysis of the PRESENT Algorithm on ATmega328P for Securing RFM95W LoRa Communications. *2024 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, 615–621. <https://doi.org/10.1109/COMNETSAT63286.2024.10862268>
- Yoga, V., Ardhana, P., Hidayat, M. T., & Jannah, M. (2023). *Implementasi RESTful API Pada Laravel dan Simulator IoT Wokwi Untuk Pengukuran Suhu dan Kelembaban Menggunakan Metode Waterfall*. 3(2), 93–109.
- Yuly, A. R., & Pradana, H. (2020). Systematic Literature Review (SLR) Development of the IoT Industry in the Southeast Asian Region. *2020 3rd International Conference on Computer and Informatics Engineering, IC2IE 2020*, 460–466. <https://doi.org/10.1109/IC2IE50715.2020.9274619>

UIN SUNAN AMPEL
S U R A B A Y A